

REMARKS

Claims 1-20 remain for consideration and are thought to be allowable over the cited art. Reconsideration and allowance are respectfully requested.

Claims 9-17 are amended for purposes of clarification and not for purposes of patentability. The amendments merely simplify the original language without changing the scope of the original claims.

The Office Action does not establish that claims 1-5 and 9-14, 16, and 17 are unpatentable under 35 USC §103(a) over “Trimberger” (U.S. patent no. 5,892,961 to Trimberger) in view of “Erickson” (U.S. patent no. 5,970,142 to Erickson et al.). The rejection is respectfully traversed because the Office Action fails to show that all the limitations are suggested by the references and fails to provide a proper motivation for modifying the teachings of the Trimberger with teachings of Erickson.

Claim 1 includes limitations of a configuration bitstream including a plurality of unencrypted words for controlling loading of configuration data in combination with a plurality of encrypted words that specify the encrypted design. This combination of limitations is not shown to be suggested by the Trimberger-Erickson combination.

Neither of Trimberger nor Erickson is shown to suggest that part of a configuration bitstream is encrypted in combination with part of the configuration bitstream being unencrypted. Trimberger teaches control words and configuration data, both being unencrypted, and Erickson is cited as teaching encrypted configuration data. Trimberger and Erickson do not, however, suggest the claimed combination of part of the configuration bitstream being unencrypted and part of the configuration bitstream being encrypted.

Trimberger teaches all of the configuration bitstream is unencrypted, both programming instructions and configuration data. Erickson does not appear to distinguish between different parts of a configuration bitstream and generally teaches configuration stream encryption (Title, Abstract). Thus, Trimberger does not encrypt anything, and Erickson appears to encrypt all of a configuration bitstream. The claimed combination sets forth that part of the bitstream is unencrypted and part of the bitstream is encrypted. Specifically, in the configuration bitstream a plurality of words for controlling loading of configuration data is unencrypted, and a plurality of words

that specify the encrypted design are encrypted. This combination is not shown to be suggested by the Trimberger-Erickson combination.

Furthermore, the alleged motivation for modifying Trimberger with Erickson for making claim 1 is improper because it lacks supporting evidence and is based on hindsight. The alleged motivation states that "it would have been obvious ... to combine a plurality of encrypted words specifying the encrypted design as per teaching of Erickson in to the method taught by Trimberger in order for securing data used to configure a PLD." No evidence is provided to indicate how the desire for securing data suggests the specific limitations of part of a configuration bitstream being unencrypted and part of the bitstream being encrypted. The general desire simply suggests encrypting data, not part of the bitstream being encrypted and part of the bitstream not being encrypted. Furthermore, in combining Erickson with Trimberger, the Office Action is simply picking and choosing selected teachings from the references without providing any evidence to support combining those selected teachings. Therefore, the alleged motivation is improper.

Claim 2 includes limitations of one of the unencrypted words comprising a key address for locating a decryption key for decrypting the encrypted words. The cited portion of Erickson alleged to suggest these limitations contains no apparent relevance to a key address being part of the unencrypted words of a configuration bitstream. The cited teaching of Erickson simply teaches using a decryption key to decrypt configuration data. There is no apparent teaching by Erickson that the decryption key is addressed by part of the configuration bitstream. If the rejection is maintained, further explanation is requested.

The alleged motivation for modifying Trimberger with Erickson for making claim 2 is improper because it lacks supporting evidence and is based on hindsight. The alleged motivation states that "it would have been obvious ... to employ the locating of the decryption key for decrypting the encrypted word as per teachings of Erickson in to the method of as taught by Trimberger for the purpose of decrypting the encrypted control words." No evidence is provided to indicate how the need to decrypt control words suggests the specific limitations of part of the unencrypted words of the bitstream including an address of a decryption key. Furthermore, in combining

Erickson with Trimberger, the Office Action is simply picking and choosing selected teachings from the references without providing any evidence to support combining those selected teachings. Therefore, the alleged motivation is improper.

Claims 3 and 4 depend from claim 1, and claim 5 depends from claim 4. These claims are not shown to be unpatentable for at least the reasons set forth above.

Independent claim 9 includes limitations similar to those of claim 1 and is not shown to be unpatentable for at least the reasons set forth above for claim 1. Claims 10, 11, 12, and 13, which depend from claim 9, and claims 14, 16, and 17, which depend from claim 1, are similarly not shown to be unpatentable over the Trimberger-Erickson combination.

The Office Action does not establish that claims 6-8 are unpatentable under 35 USC §103(a) over Trimberger in view of Erickson, in further in view of "Kwiat" (U.S. Patent 5,931,959 to Kwiat). Claims 6, 7, and 8 depend from claim 1 and are patentable over the Trimberger-Erickson-Kwiat combination for at least the reasons set forth above. In addition, the rejection is respectfully traversed because the Office Action fails to show that all the limitations are suggested by the references and fails to provide a proper motivation for modifying the teachings of the Trimberger-Erickson combination with teachings of Kwiat.

Furthermore, Kwiat merely suggests computing a CRC code. However, there is no apparent suggestion of any order of computing a CRC code relative to encrypting the configuration data as set forth in claims 7 and 8. Further clarification is requested if the rejection is maintained. Otherwise the rejection should be withdrawn.

The alleged motivation states that "it would have been obvious ... to combine a Cyclic redundancy checksum (CRC) as per teaching of Kwiat in to the method of as taught by the combination of Trimberger and Erickson, in order to increase the chance of providing error free configuration of the PLD or FPGA when the design in the form of bitstream is loaded on to the PLD or FPGA." It is respectfully submitted that this alleged motivation has no apparent relation to the order of computing a CRC code relative to encrypting the configuration data as set forth in claims 7 and 8. Thus, the alleged motivation is improper.

The rejection of claims 6-8 over the Trimberger-Erickson-Kwiat combination should be withdrawn because the Office Action fails to show a suggestion of all the limitations and fails to provide a proper motivation for combining the references.

The Office Action does not establish that claim 15 is unpatentable under 35 USC §103(a) the Trimberger-Erickson combination in further in view of "Yin" (U.S. Patent 6,028,939 to Yin). Claim 15 depends from claim 1 and is patentable over the Trimberger-Erickson-Yin combination for at least the reasons set forth above. In addition, the rejection is respectfully traversed because the Office Action fails to show that all the limitations are suggested by the references and fails to provide a proper motivation for modifying the teachings of the Trimberger-Erickson with teachings of Yin.

Claim 15 includes limitations of the plurality of unencrypted words for controlling loading of configuration data include a cipher block chaining initial value. Yin is cited as suggesting these limitations. However, Yin simply teaches general use of cipher block chaining. There is no suggestion of the further limitations of the initial value being in unencrypted words of configuration data. Thus, the Office Action fails to show that the combination suggests the limitations of claim 15.

The alleged motivation is improper because it is unsupported by evidence. The alleged motivation states that "it would have been obvious ... to employ the inclusion of cipher block chaining initial value as per teachings of Yin in to the method of as taught by the combination of Trimberger and Erickson for the purpose of strengthening the security of the PLD since a single bit error in a ciphertext block affects the decryption of all subsequent blocks." This alleged motivation contains no evidence of a motivation to include the cipher text block initial value in the unencrypted words for controlling the loading of configuration data. The alleged motivation simply states a general use for ciphertext encryption without providing any evidence to motivate the specific inclusion of the initial value in the unencrypted data. Therefore, the Office Action fails to establish that claim 15 is unpatentable over the Trimberger-Erickson-Yin combination.

The Office Action does not establish that claims 18-20 are unpatentable under 35 USC §103(a) over Erickson in view of Yin. The rejection is respectfully traversed because the Office Action fails to show that all the limitations are suggested by the references and fails to provide a proper motivation for modifying the teachings of Erickson with teachings of Yin. No suggestion is shown of forming a cipher block chaining initial value comprising a starting address for loading a design into a PLD. None of the cited teachings in either of the references appear to reference this specific use of the starting address.

The Office Action also fails to provide a proper motivation for combining Yin with Erickson. The alleged motivation states that "it would have been obvious ... to encrypt the control word in chain block mode as per teachings of Yin in to the encryption method as taught by Erickson in order to enable a cost-effective, scalable and high performance implementation of data security." The alleged motivation fails to provide any evidence that Erickson is not cost effective, not scalable, and not high-performance. Furthermore, the general objectives of cost-effectiveness, scalability and high performance do not in any apparent way motivate the specific limitations of forming the initial cipher block chaining value comprising the starting address. Therefore, the alleged motivation is unsupported by evidence and improper.

Claims 19 and 20 depend from claim 18 and are patentable over the Erickson-Yin combination for at least the reasons set forth above. The Office Action does not establish that claims 18-20 are unpatentable over the Erickson-Yin combination, and the rejection should be withdrawn.

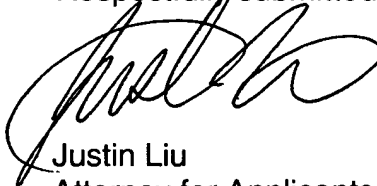
Information Disclosure Statement

Applicants have not yet received signed copies of the Information Disclosure Statements filed on October 15, 2004, January 14, 2005, and January 31, 2005. Applicants respectfully request copies of the initialed and signed substitute forms 1449A.

CONCLUSION

Reconsideration and a notice of allowance are respectfully requested in view of the Remarks presented above. If the Examiner has any questions or concerns, a telephone call to the undersigned is invited.

Respectfully submitted,



Justin Liu
Attorney for Applicants
Reg. No.: 51,959
(408) 879-4641

I hereby certify that this correspondence is being deposited with the United States Postal Service as first-class mail in an envelope addressed to: Commissioner for Patent, P.O. BOX 1450, Alexandria, VA 22313-1450, on August 8, 2005.

Julie Matthews
Name


Signature